Information Security and Cyber Risk Management

October 2022

ZURICH®

Advisen
A ZYWAVE COMPANY

Contents

Introduction

The past few decades have seen a substantial rise in cyber risk awareness and the growing need for cyber insurance. Our 12th annual Information Security and Cyber Risk Management Survey reflects that growing awareness: It found that 86 percent of respondents have cyber insurance, with 69 percent holding standalone policies—up three percentage points from last year's findings on both fronts and the highest numbers to date since the inception of the survey. The survey also revealed some intensifying challenges. Specifically, this year's results depict a risk manager and insurance buying market that is facing difficulties navigating higher premiums, shrinking capacity, reduced coverage and altered policy language brought on by the rising frequency and severity of claims, growing attacker sophistication and prevalence of new threats.

While some understand the factors influencing the need for cyber coverage adjustments, others have struggled with the extent of the impacts on insurance costs, policy clarification and risk selection. As such, our latest survey findings emphasize the importance of risk managers and their insurance partners working hand-in-hand to promote a greater understanding of the links between market dynamics, actions to improve resilience and accessibility of coverage.

This year's results indicate some signs of progress in building cyber resilience, with the vast majority of respondents having taken steps to assess their risk and invest in related solutions. Yet, there is still room for improvement. Less than two-thirds of respondents confirmed that their organization's risk managers and IT professionals work together to monitor cyber risk. Additionally, while more than three-quarters of respondents reported having cyber incident response plans, a significantly smaller group tests these plans regularly. Furthermore, despite many respondents listing employee training as a high priority, just two-thirds offer this training one or more times a year.

These shortcomings highlight key areas where risk managers and their insurance providers can work together to offer much-needed education and support on the road to resilience. Such preparation can also help risk managers better demonstrate proper cybersecurity measures to underwriters—an increasingly critical (and sometimes mandatory) practice.

In terms of key exposures, Cyber Extortion/Ransomware and Data Breach remain top coverage expectations among organizations, as these events have surged in recent years. Apart from these exposures, ongoing global geopolitical conflicts have prompted some organizations to reassess their cyber coverage needs and risk mitigation measures in anticipation of elevated nation-state threats. Such conflicts have also posed questions regarding which parties are responsible for handling losses from cyberwarfare. Against this backdrop, insurers are calling for increased public-private partnership to address the prospect of large-scale, nation-state cyberattacks, which may cause losses too deep for organizations and insurers to absorb.

Especially as cyber exposures shift and the market fluctuates, it's vital for organizations to focus on what they can control—such as identifying critical assets, assessing potential vulnerabilities, creating protective security procedures and adopting policies that can help support business continuity after various cyber incidents. When organizations, risk managers and their insurance providers take a collaborative, proactive approach to managing possible threats, they can truly make a difference in preventing and mitigating cyber losses.

Survey Highlights

86 percent of respondents have cyber insurance, the highest percentage to date in the 12 years of the survey and up three percentage points from 2021.

- Despite rising awareness of the frequency and cost of cyber incidents and the growing sophistication of perpetrators, some cyber insurance buyers have expressed frustration with rate increases, changes in coverage availability and policy terms. While the majority of respondents still view cyber coverage as a valuable purchase, some had harsh words for insurance providers.

- 54 percent of respondents who experienced a claim reported it to their cyber insurance carrier. More than 70 percent recouped costs from their cyber insurance carrier, while a portion of claims are still in process.

- Nearly all (94 percent) of respondents selected Data Breach as a form of coverage they expect to be included within their cyber policies. Cyber Extortion/Ransomware remains close behind at 93 percent, followed by Data Restoration at 87 percent, Business Interruption at 75 percent, System Failure at 72 percent and Bricking at 70 percent.

- 62 percent of respondents cited enhancing employee training as one of their top cybersecurity priorities over the next year, followed by conducting a cybersecurity assessment/audit/gap analysis (58 percent) and doing a tabletop exercise (49 percent).

- Though employee training was listed as a priority, one-quarter of respondents reported offering this training only on an annual basis, with just 19 percent offering it twice a year and 22 percent offering it quarterly.

- 81 percent of respondents have cyber incident response plans in place, while nearly 60 percent test these plans regularly and for multiple scenarios. Even though all organizations should have such plans, this year's findings represent progress over previous years.

- The vast majority of respondents (83 percent) reported that cyber risk poses a significant concern for their organizations and have taken steps to assess their risk. Additionally, 69 percent have invested in cybersecurity solutions to mitigate risk, and 60 percent confirmed that risk managers and IT professionals work together to monitor such risk.

- When asked to rank a list of business continuity concerns posed by cyber events, respondents rated almost all of them as a medium- to high-risk, with the concern of their networks being held hostage for extortion selected as the highest risk. This concern was followed by business interruption, cloud vulnerabilities, distributed denial-of-service (DDoS) attacks, and contingent business interruption.

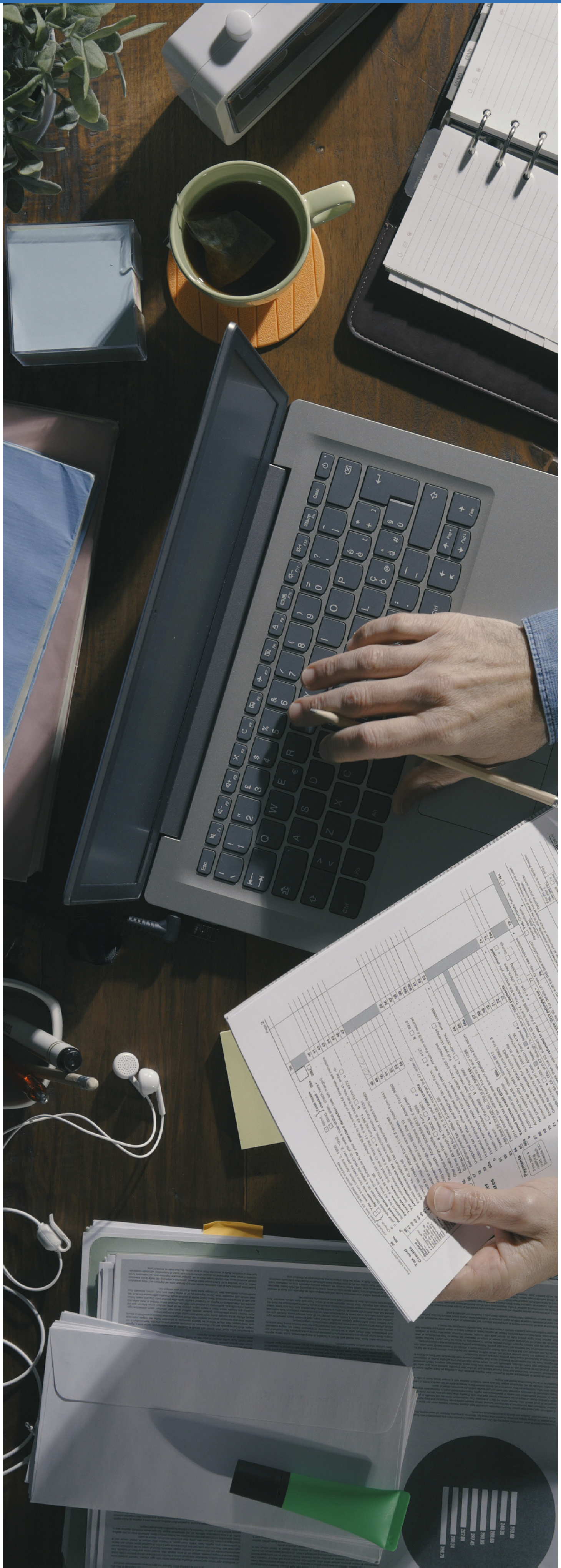
- In terms of data integrity risk, respondents ranked malware/ransomware as their top concern, followed by employees unintentionally infecting their organizations' networks and data breaches. Reputational risk tied to the loss of customer data also ranked high.

Survey Highlights (cont.)

- The percentage of respondents who agreed their cyber insurance policies are written in a clear and easy-to-understand manner gained ground in 2022. Yet, one-third of respondents still disagreed or completely disagreed with this statement—down from 37 percent in 2021, 34 percent in 2020 and 40 percent in 2019.

- More than half (52 percent) of respondents agreed that their cyber insurance meets organizational needs and provides value, while 61 percent said their coverage meets some but not all organizational needs.

- Analysis of the results tracked a fairly high level of “don’t know” answers to many questions. As such, those responsible for managing their organization's cyber risk may use this survey for insights to close awareness gaps and methods to increase their resilience.



Perceptions of Risk

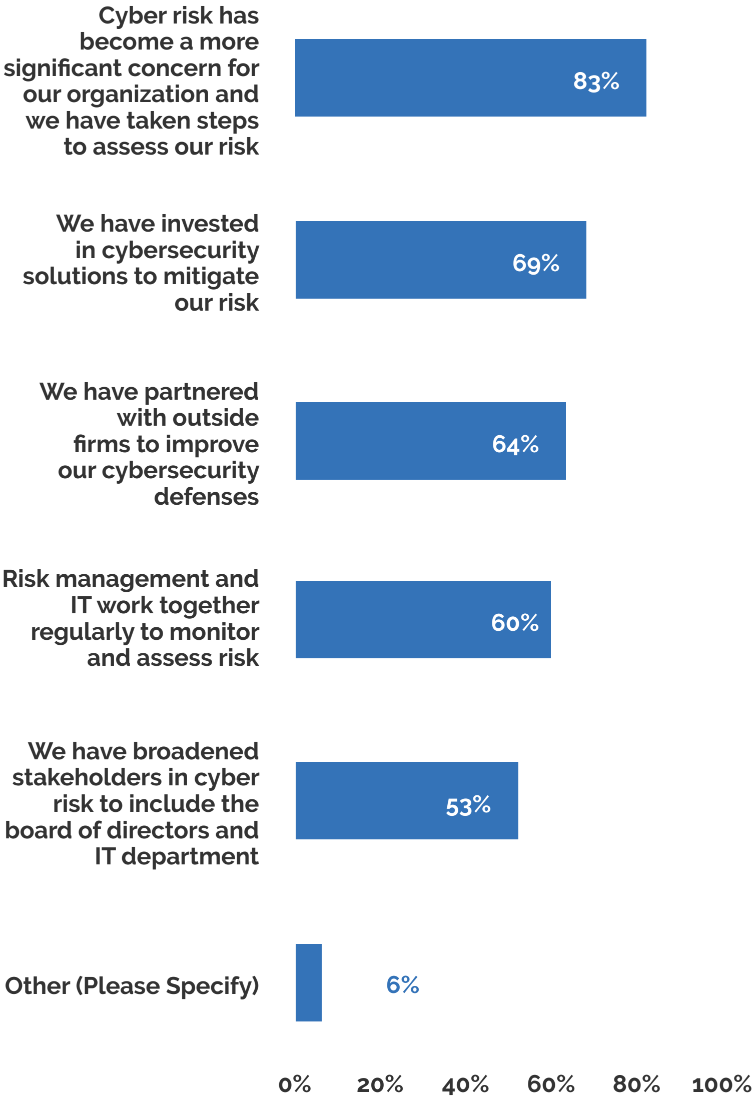
Organizations have become increasingly aware of the wide variety of cyber exposures they face, elevating risk management as a priority. This year's findings confirmed that the vast majority of respondents (83 percent) believe cyber risk is a significant concern for their organizations and that steps have been taken to assess their risk. Additionally, 69 percent of respondents have invested in cybersecurity solutions to mitigate their risk, and 60 percent confirmed that risk managers and IT professionals work together to monitor such risk.

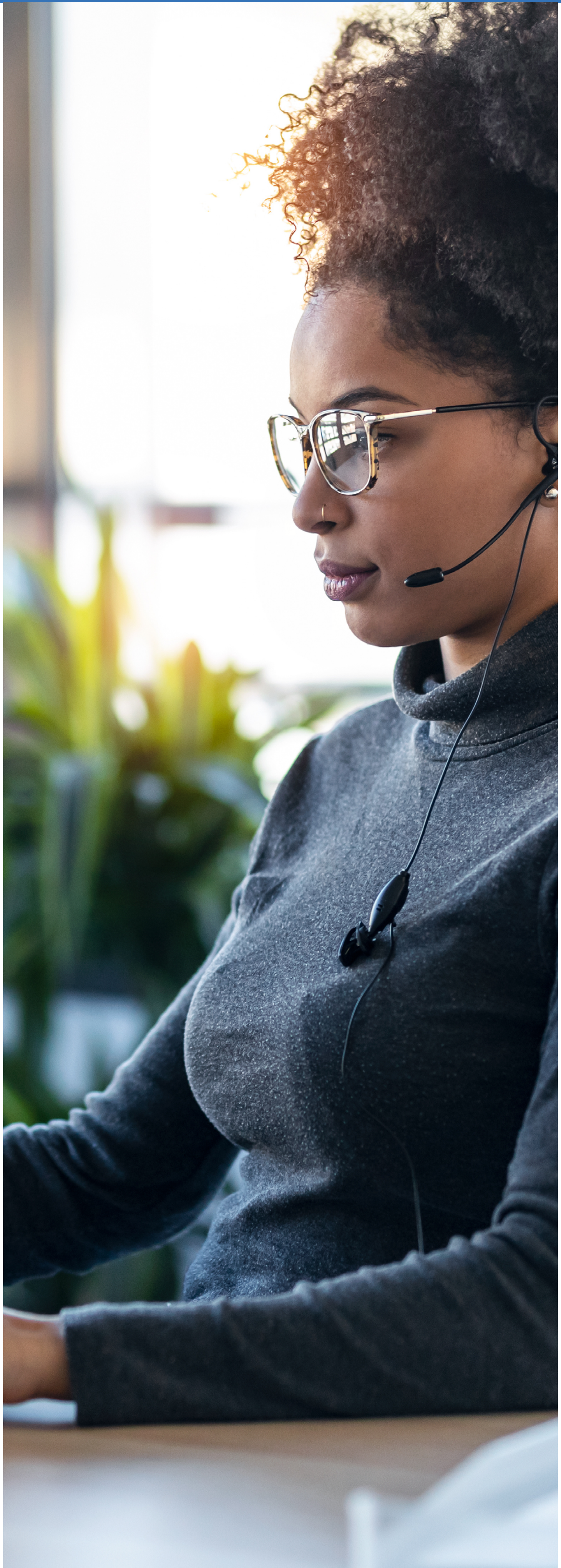
Some organizations have also sought help from external parties to address cyber threats. Nearly two-thirds (64 percent) of respondents have partnered with outside firms to bolster their cybersecurity posture. In comparison, 53 percent have expanded cyber stakeholders in their organization to include board members and the IT department. While these are generally positive trends, they closely mirror last year's findings—suggesting some stagnation.

Certain comments from respondents on this topic clarify the challenges companies face today, with one respondent stating their organization had completed none of the provided options to manage their cyber risk and had instead adopted a "siloed ostrich approach." Another respondent cited a "difficult relationship" with IT and cyber risk management colleagues. One respondent classified cybersecurity as an "annual strategy." Although this comment suggests that cybersecurity is being viewed as a strategic investment, addressing cyber exposures far more frequently than once a year is critical to ensure sufficient protection.

When it comes to cybersecurity goals for the next year, employee training is top-of-mind for many organizations, with 62 percent of respondents seeking to enhance such training going forward. Despite this, one-quarter of respondents reported offering employee training only on an annual basis, whereas

How has your organization's approach to cyber risk management evolved over the years? (Please select all that apply)



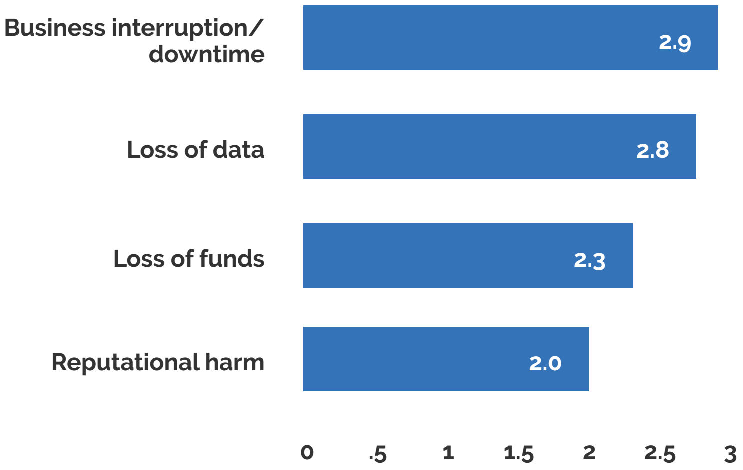


just 19 percent offer it twice a year and 22 percent offer it quarterly. Apart from enhancing employee training, more than half of respondents (58 percent) plan to conduct a cybersecurity assessment/audit/gap analysis in the next year, while 49 percent are looking to perform a tabletop exercise.

Regarding business continuity risk, respondents considered having their networks held hostage for extortion as the greatest concern. This concern was followed by business interruption, cloud vulnerabilities, DDoS attacks, and contingent business interruption. Notably, respondents rated almost all provided business continuity concerns posed by cyber events as a medium- to high-risk, with the exception of property damage/bodily injury.

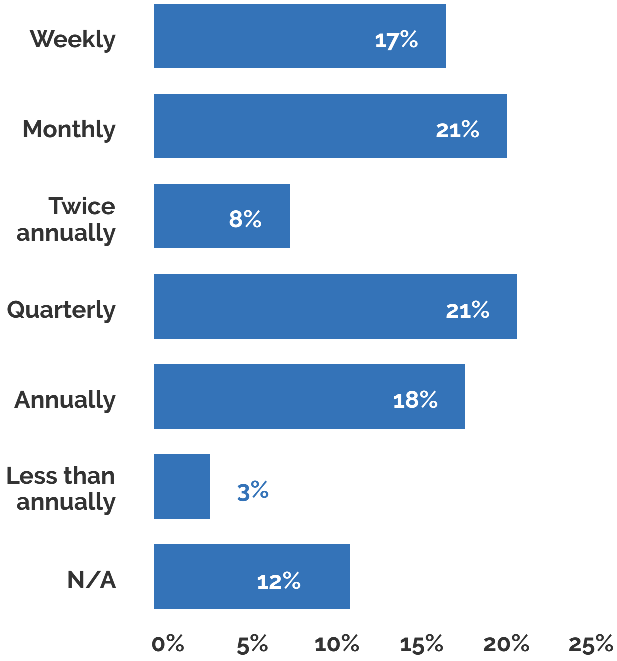
As it pertains to data integrity risk, respondents ranked malware/ransomware as their top concern, followed by employees unintentionally infecting their organizations' networks and data breaches. Nonetheless, while Data Breach is the top form of coverage respondents expect to be included within their policies, more than one-third (39 percent) consider business interruption to be the worst possible outcome of a cyber event—followed by loss of data (24 percent), loss of funds (21 percent) and reputational harm (17 percent).

Please rank the following outcomes of a cyber event starting with the worst outcome.



Despite these concerns, most respondents say that their organizations are equipped to handle potential cyber incidents. The majority of respondents said they are either moderately (43 percent), very (41 percent) or extremely (6 percent) prepared for a cyber event. In comparison, 62 percent confirmed they are either moderately or extremely prepared for a supply chain incident. Such confidence may partially stem from the growing proportion of organizations that have adopted cyber incident response plans. More than three-quarters of respondents (81 percent) have such plans in place, and nearly 60 percent test these plans regularly and for multiple scenarios. Almost half (48 percent) of respondents developed their cyber incident response plans with the help of cybersecurity vendors, and 46 percent of respondents received assistance from internal parties. Only 17 percent sought help from their insurance providers—highlighting a potential growth opportunity for carriers and brokers.

How often do you assess your company's exposure to cyber risks based on the current threat environment?



While developing incident response plans is an important step in building cyber resilience, this year's results indicate that more work still needs to be done. Namely, organizations need to make a conscious effort to analyze their cyber risk on a more regular basis. Of respondents that assess their cyber exposures, 21 percent do so quarterly, another 21 percent do so monthly, and 18 percent do so only annually. Organizations that keep closer tabs on their specific exposures and respond accordingly may be less likely to experience devastating cyber events.

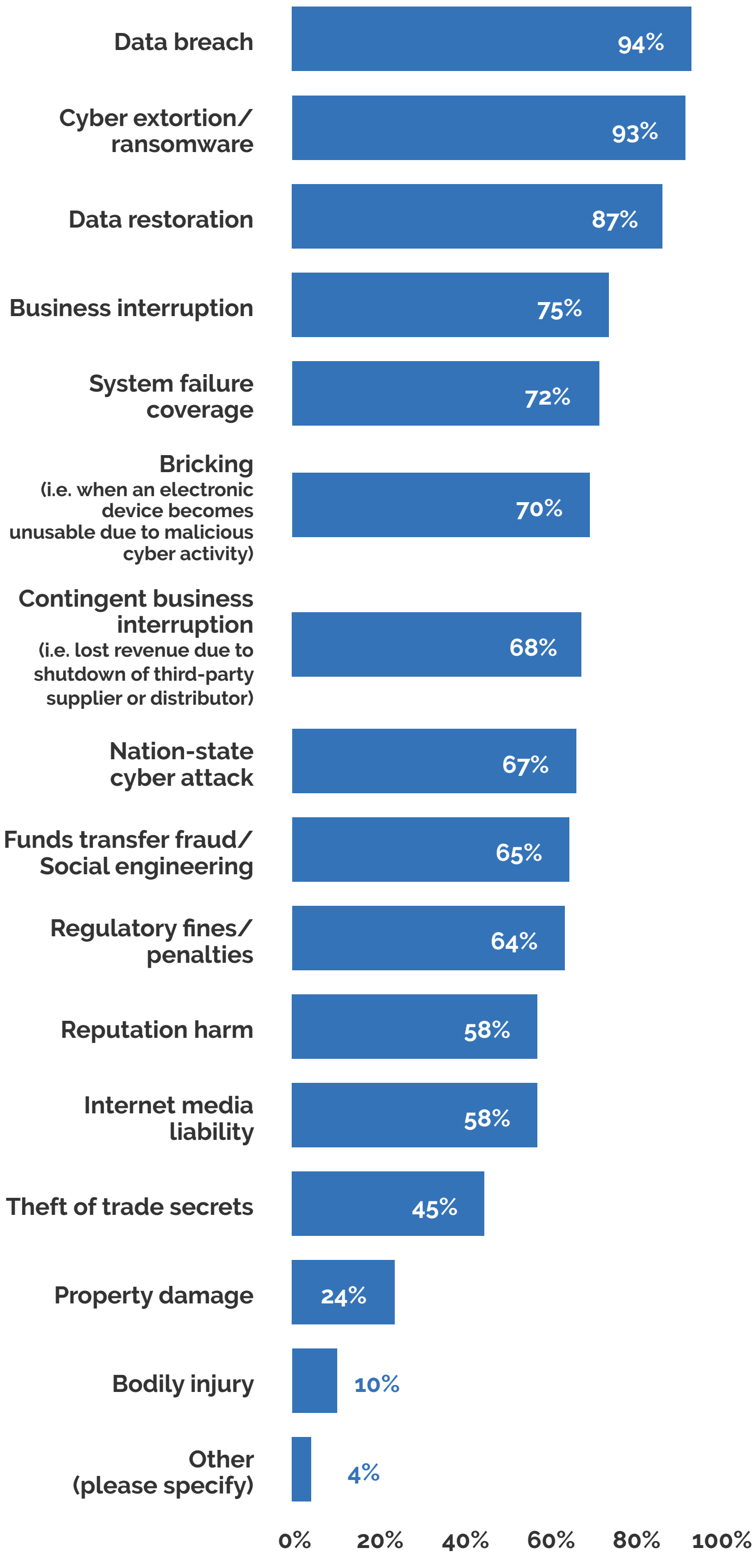
Perspectives on Insurance

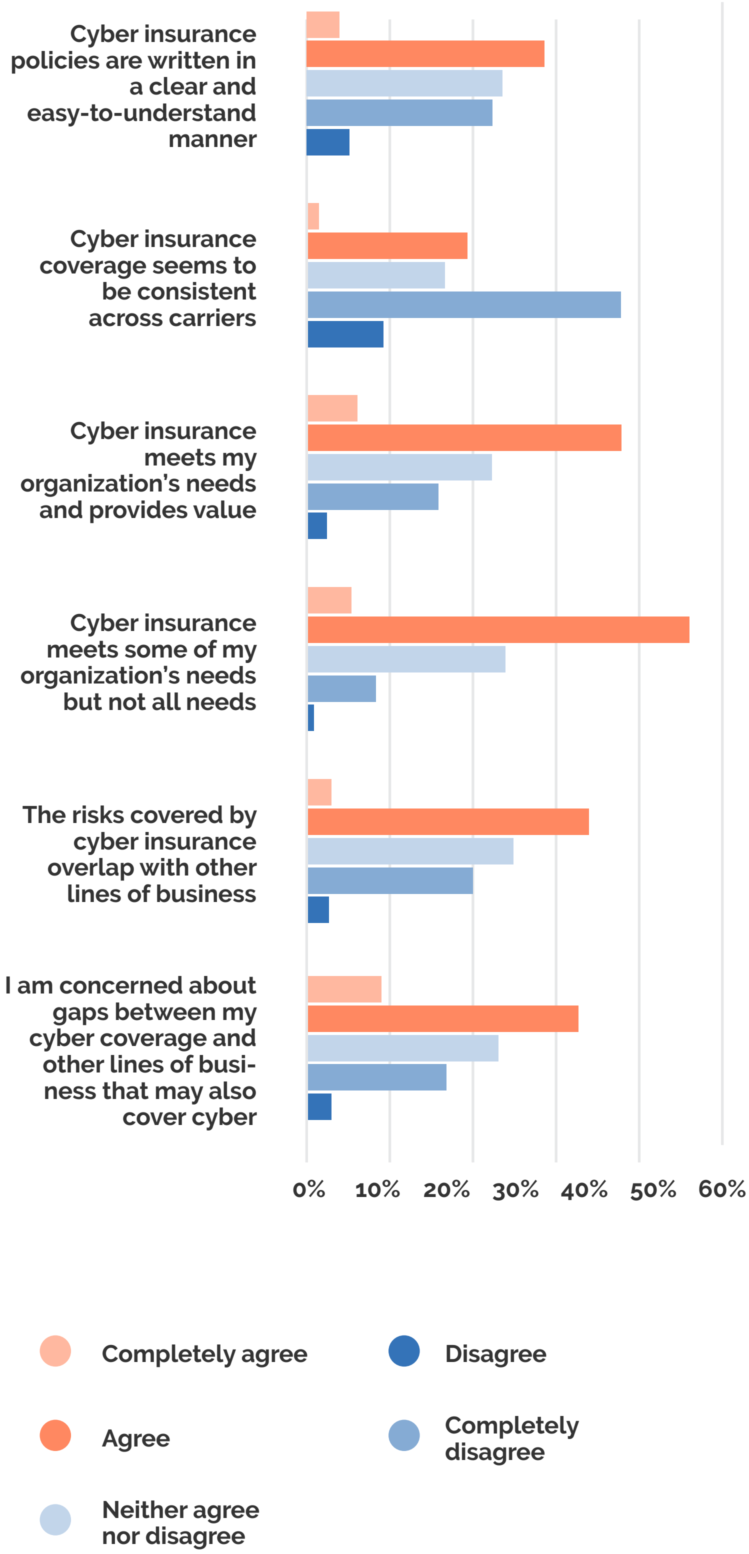
As a growing number of organizations faced ransomware attacks and data breaches in recent years, insurance buyers' coverage expectations followed suit. This year's results saw Data Breach take the lead as a form of coverage respondents expect to be included within their cyber policies, with 94 percent expecting such coverage. Cyber Extortion/ Ransomware remains close behind at 93 percent, followed by Data Restoration at 87 percent, Business Interruption at 75 percent, System Failure at 72 percent and Bricking at 70 percent.

Apart from these types of coverage, respondents also displayed a clear desire for additional insurance offerings, including Contingent Business Interruption (68 percent) and Nation-state Cyberattacks (67 percent). What's more, at least half of all respondents selected the vast majority of coverage expectation options, with the exception of Theft of Trade Secrets (45 percent), Property Damage (24 percent) and Bodily Injury (10 percent). Multiple respondents commented that their coverage expectations include "all of the above," thus referencing every option provided.

The percentage of respondents who said their cyber insurance policies are written in a clear and easy-to-understand manner gained ground this year, with 39 percent agreeing or completely agreeing with this statement and 28 percent neither agreeing nor disagreeing. One-third of respondents still disagreed or completely disagreed with this statement—down from 37 percent in 2021, 34 percent in 2020 and 40 percent in 2019.

What do you expect a cyber insurance policy to cover? (Please select all that apply)





Insurance carriers' differences in appetite for cyber exposures and varied approaches to addressing systemic risk in portfolios have likely affected policy consistency; a rising proportion of insurance buyers noted this. Specifically, more than half (56 percent) of respondents disagreed or completely disagreed that cyber coverage is consistent across insurance carriers, representing an increase of two percentage points from the previous year.

In the scope of managing coverage gaps and overlaps, this year's findings demonstrate that progress may have stalled from prior years. Nearly half (49 percent) of respondents said they are concerned about gaps between their cyber coverage and other insurance products that may also provide such coverage—the same percentage as in 2021, although down from 54 percent in 2020. In addition, 44 percent of respondents said they have noticed overlaps in coverage between their cyber insurance and other insurance products. This is an increase from 2021 (39 percent), yet a decrease from 2020 (48 percent).

Perhaps more concerning is the proportion of respondents who neither agreed nor disagreed with statements regarding cyber coverage gaps (27 percent) or overlaps (30 percent), which remained relatively unchanged from 2021. As mentioned in last year's results, this level of indifference seems particularly high for an issue with potentially severe consequences. Such indifference could have significant financial ramifications among organizations that experience cyber losses and discover they lack sufficient coverage. Amid a challenging cyber insurance market, it's possible that risk managers may be more concerned with simply securing some level of coverage rather than ensuring robust protection for their organizations. But, between this year's findings on policy inconsistency and today's increasingly litigious environment, attention to coverage gaps and overlaps is critical to help prevent major out-of-pocket losses.

When asked about satisfaction with their cyber insurance, respondents had mixed perspectives. Although 52 percent of respondents either agreed or completely agreed that their coverage meets their expectations and provides value, 61 percent said their policies meet some—but not all—of their organizational needs. These findings represent shifts from 57 percent and 55 percent in 2021, respectively. Further, a discouraging finding is that 22 percent of respondents either disagreed or completely disagreed that their cyber insurance meets expectations and provides value, while 26 percent neither agreed nor disagreed.

As a whole, this year's results indicate that some insurance buyers remain uncertain of the value of cyber coverage. This may be influenced by the fact that the coverage is relatively new and evolving more rapidly than other forms of insurance as market exposures continue to shift and expand. Many other lines of coverage have historically been less dynamic after their initial introduction (e.g., the workers' compensation market following the Industrial Revolution).

In any case, the ever-changing cyber risk landscape requires increasing sophistication from insurance buyers year over year. This presents the opportunity for cyber insurance carriers and brokers to provide continued education and updates on the risk environment and related cyber threat mitigation techniques, fostering greater market understanding.

> More than half of respondents **disagreed** or **completely disagreed** that cyber coverage is consistent across insurance carriers.

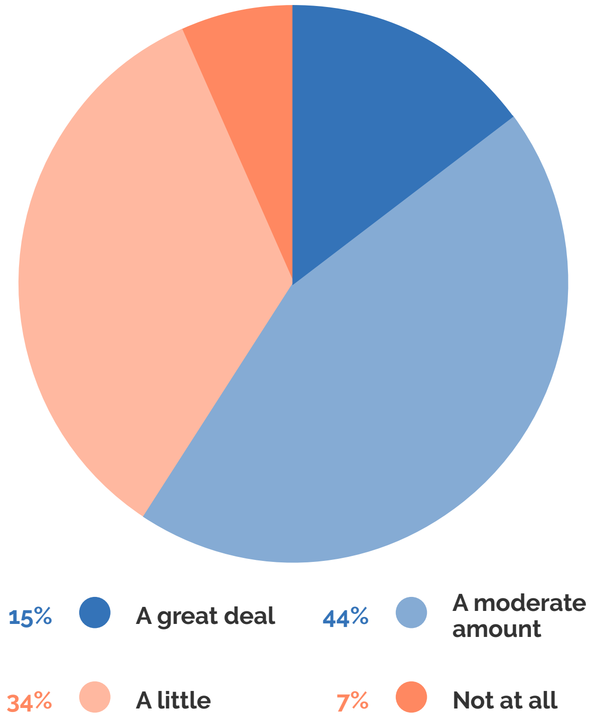
Geopolitical Conflict in Focus

Geopolitical conflict over the past year has elevated cybersecurity concerns, particularly regarding the imbalance between sophisticated cyber weapons employed by nation-states and the defense tools that are commercially available. Amid fears of cyberwarfare, this year's survey included a new section prompting respondents to discuss how geopolitical conflict has affected their organization's cybersecurity decisions.

The majority of respondents reported some level of concern about geopolitical conflict and its impact on the cyber risk landscape. In particular, 44 percent of respondents said these conflicts have affected their views of cyber risk a moderate amount, 34 percent said these conflicts have impacted their views a little, and 15 percent said such conflicts have affected their views a great deal, while 7 percent said their views have not been impacted whatsoever.

To address geopolitical conflict concerns, more than half (52 percent) of respondents have increased their organizations' oversight of IT vendor management. More than one-third of respondents have reviewed guidance from the Cybersecurity Infrastructure and Security Agency (CISA) or other federal agencies (39 percent), identified critical suppliers (38 percent) or assessed network connectivity with vendors (36 percent). Although respondents were asked to respond with geopolitical conflict in mind, it's worth noting that these measures can help map and minimize cyber risk across the board for organizations—especially in terms of vendor-related exposures and supply chain threats.

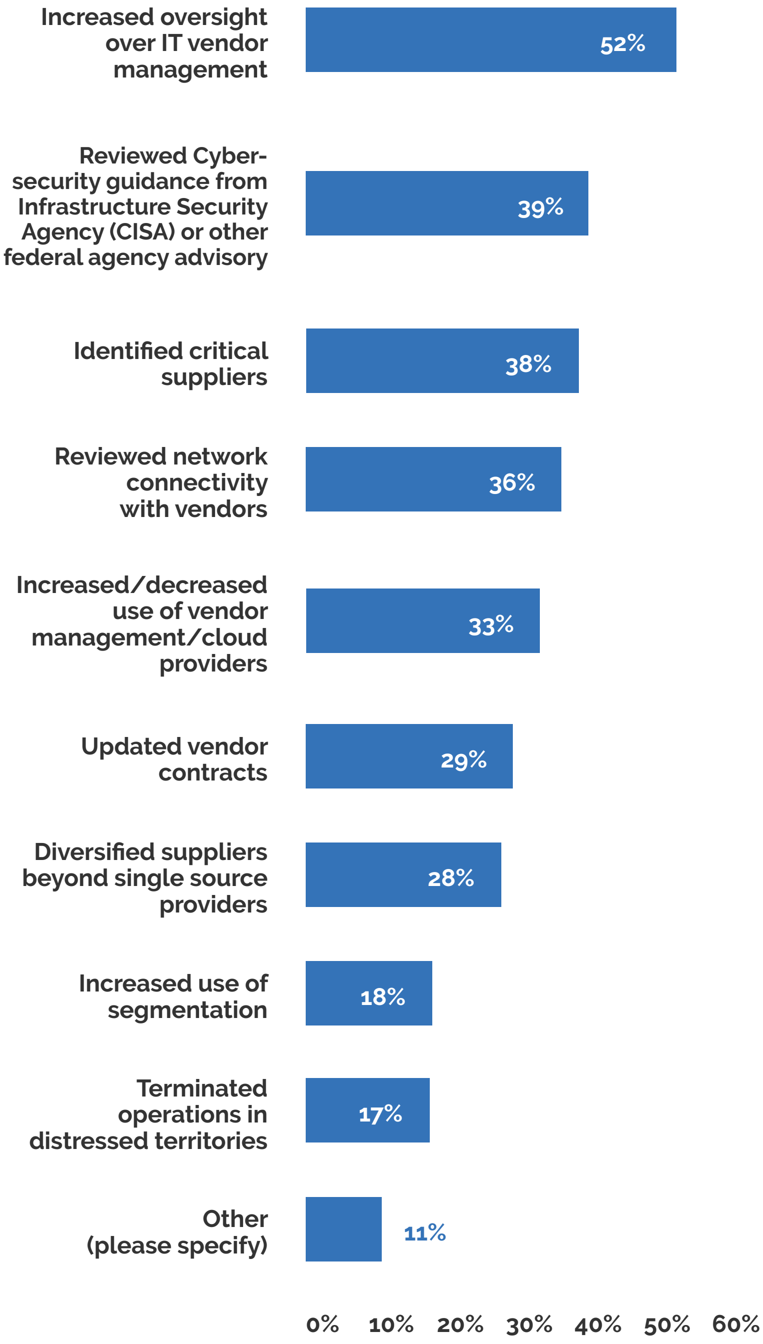
Does the current geopolitical conflict(s) impact your view of cyber risk?



While a sizeable proportion of respondents said they have taken steps to reduce potential exposures stemming from geopolitical conflict, others shared that they either haven't or don't know whether they have made related cybersecurity adjustments. Some respondents' comments framed cyber risk brought on by such conflict as "nothing new" for their organizations, suggesting the possibility of exposure blind spots and less mature approaches to cybersecurity as a whole or, by contrast, a significant amount of sophistication and foresight.

Respondents seemed disinclined to increase their cybersecurity spending based on geopolitical conflict, with 57 percent reporting that they have not made any changes to their organizations' cyber-related investments due to such conflict. One-fifth (20 percent) of respondents increased their cybersecurity spending by less than 25 percent, while just 3 percent increased their investment. Only 2 percent of respondents decreased their investment, and 20 percent were unsure whether their organizations had made any cyber-related investment changes.

What, if any, changes has your organization made as a result of geopolitical conflict concerns? (Select all that apply)



Respondents who made no changes in their organization's cybersecurity spending due to geopolitical conflict offered a range of reasons. One respondent said, "We feel that we need to be protected from attacks from wherever they come at any time. The geopolitical climate just increases the frequency of attack." Other respondents asserted that they had increased their cybersecurity spending due to factors extending beyond geopolitical conflict.

Another respondent cited cyber insurance restrictions and how they may impact coverage for losses stemming from geopolitical conflict and nation-state threats (e.g., cyberwarfare). "Geopolitical conflict is the basis for many more cyberattacks," said one respondent. "Reworded war exclusions and trade/economic sanctions compliance diminishes an insurer's ability to cover loss on behalf of its insureds." Such a comment raises important questions. Specifically, if we rely on the government to defend and protect us from the use of large-scale physical weapons (e.g., bombs) launched by international actors and assist with financial remediation, who should be responsible for handling the financial damage that results from cyberweapons deployed by nation-states? Furthermore, what is the private sector's recourse to this activity?

Because nation-state cyber threats are often linked to supply chain incidents, respondents were also prompted with questions regarding their organization's third-party risk. Namely, when asked what actions they have undertaken to tighten cybersecurity controls following high-profile events involving the digital supply chain, a concerning proportion of respondents replied "none" or "don't know."

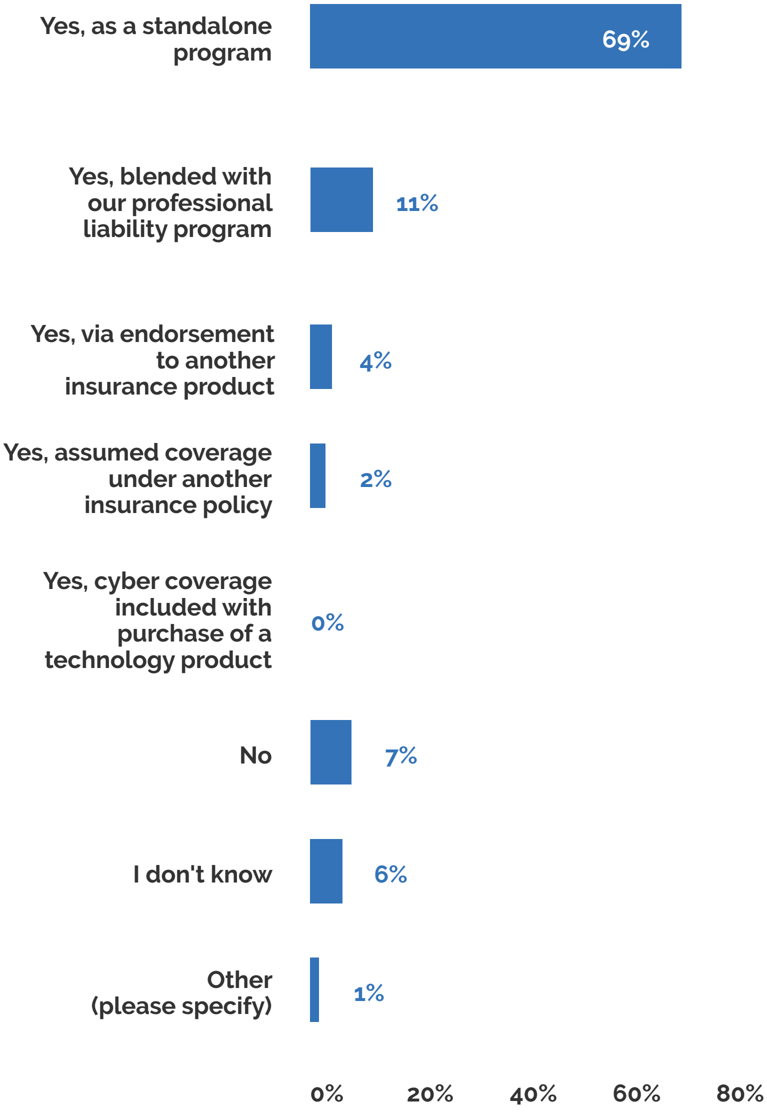
Even though some of these answers came with the caveat that actions had already been taken or were previously considered within existing cybersecurity efforts, several comments indicated a pattern of respondents thinking they were not at risk or lacking ample knowledge of third-party exposures. While 62 percent of respondents believe their organizations are either moderately or extremely prepared for a supply chain incident, limited awareness regarding third-party risk paints a different picture. Looking ahead, as geopolitical conflict concerns and associated nation-state threats persist, it's vital for organizations, risk managers and their insurance providers to work together to better understand and safeguard themselves against potential supply chain exposures.

Still Buying, but Questioning Pricing and Conditions

As previously mentioned, uptake for cyber insurance continues to grow, with 86 percent of respondents having purchased such coverage—up three percentage points from 2021 and representing the highest percentage since the inception of the survey 12 years ago. Organizations have also increasingly moved toward standalone cyber coverage. More than two-thirds (69 percent) of respondents said they have standalone policies, up from 66 percent in 2021 and 55 percent in 2020.

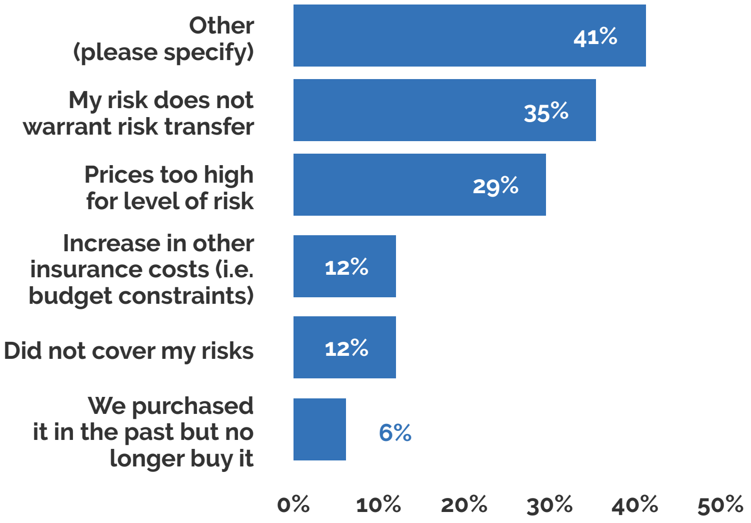
As for those who haven't secured standalone coverage, 11 percent of respondents have cyber insurance blended within their professional liability programs. Meanwhile, 4 percent have protection via endorsement to another insurance product, and 2 percent have assumed coverage through different policies. Among respondents with cyber coverage endorsements, 75 percent have an endorsement connected to their general liability policies, while 25 percent have an endorsement under their directors and officers policies .

Does your company currently purchase cyber coverage?



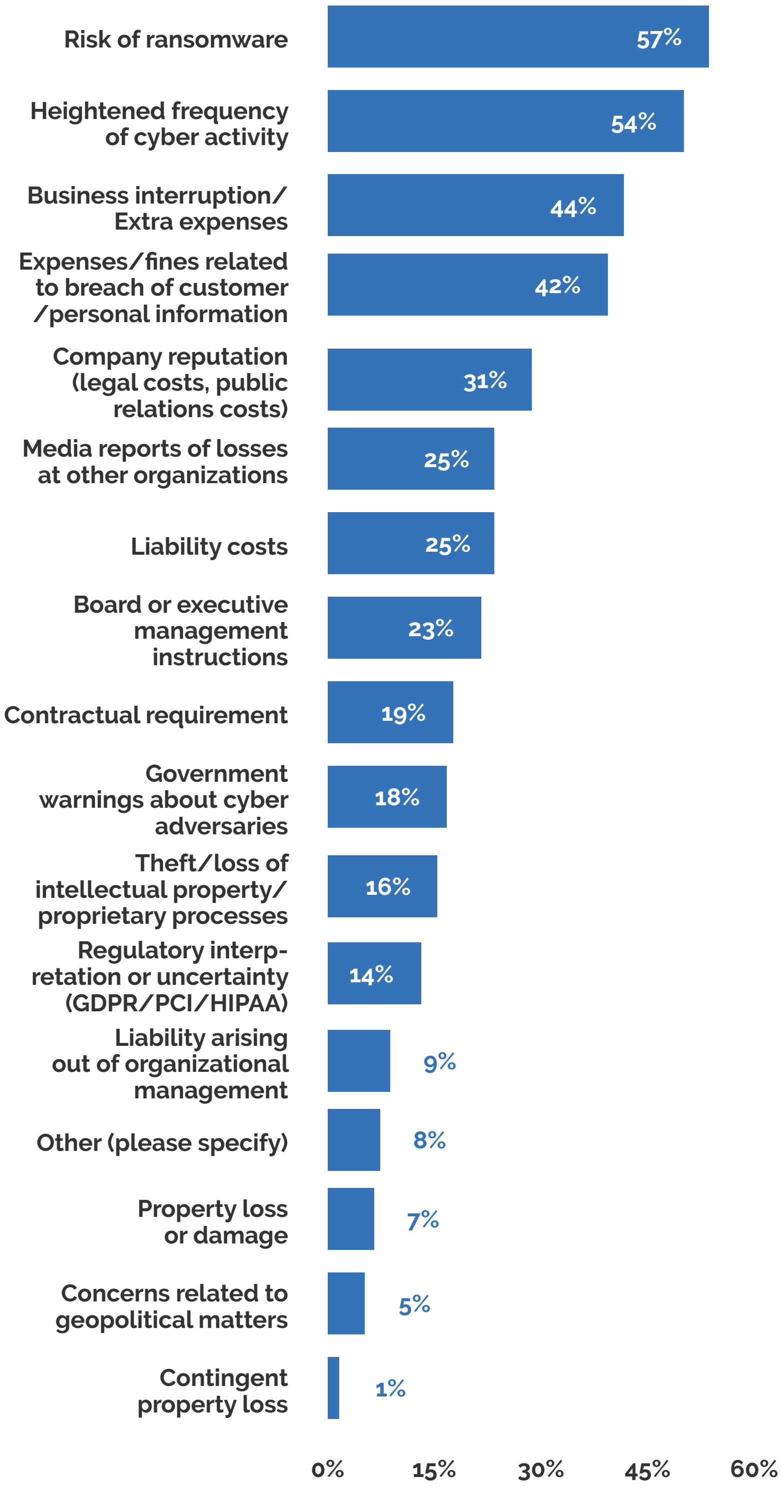
An additional 7 percent of respondents don't carry cyber coverage whatsoever, and 6 percent are unsure whether they do. More than one-quarter (29 percent) of respondents without cyber insurance cited the high cost of such coverage as their reason (down from prior years), while 35 percent attributed this decision to their organizations' cyber exposures not warranting risk transfer. Yet, 41 percent of respondents who lack coverage selected "other" as their reason for not obtaining a policy. Within this category, respondents specified various factors behind their decision, including a preference for self-insurance, lack of interest and having been able to successfully "bounce back" from previous cyber events without coverage.

Why did your company choose not to purchase cyber insurance? (Select all that apply)



Although 2015 and 2019 brought the most new buyers into the cyber insurance market, the market still saw some growth over the past year. There are many reasons why respondents have opted to purchase cyber coverage. In prior years, expenses and fines related to a breach of customer or personal information were key motivations for securing policies. Today, more than half (57 percent) of respondents said the risk of ransomware is now their primary motivator, with the expenses and fines factor falling to fourth place (42 percent). Respondents also selected a heightened frequency of cyber activity (54 percent) and business interruption/extra expenses (44 percent) as reasons for purchasing coverage. Some respondents commented that they decided to invest in coverage after receiving guidance from their brokers or having cyber exposures removed from the scope of their general liability policies.

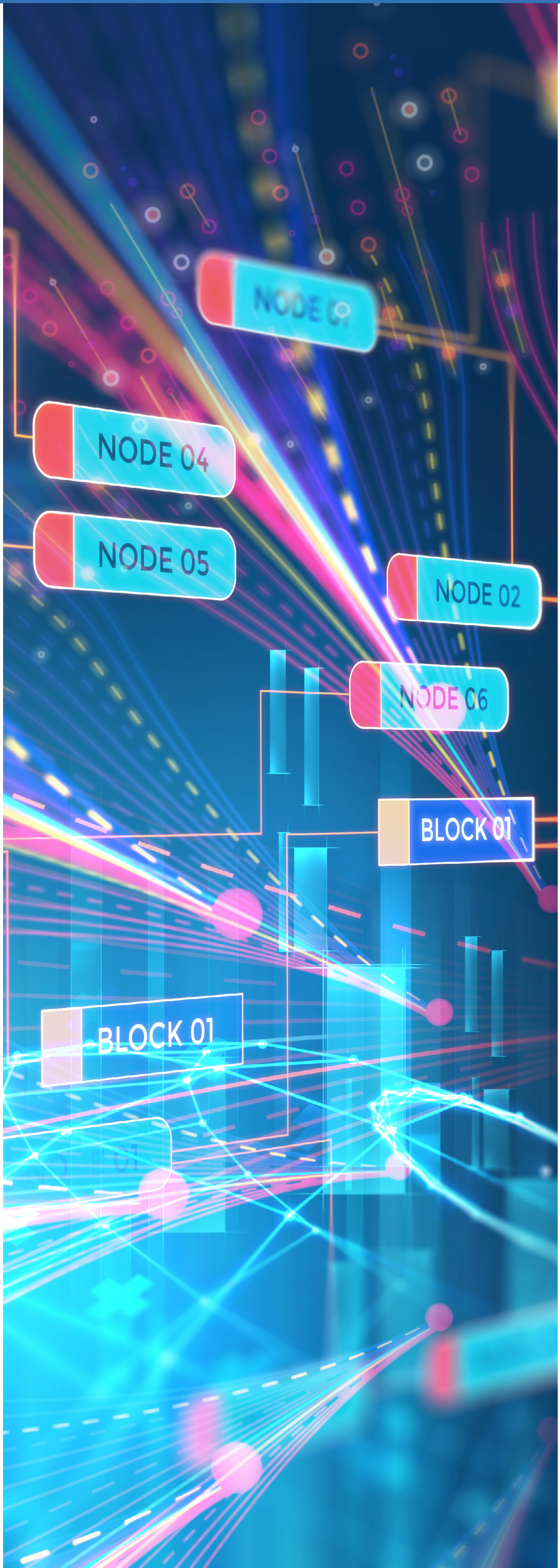
What were the primary reasons for purchasing this type of coverage? (Please choose top three)



Nevertheless, ongoing hard market conditions in the cyber insurance space have left many respondents unsatisfied with the product. Respondents commented that the market has become "frustrating and unpredictable" as well as "fragmented and non-cohesive." What's more, even though the majority of respondents still consider cyber insurance to be a valuable purchase, some are questioning the sustainability of the market, breadth of coverage offerings and broker knowledge. One respondent commented, "The cost seems to be increasing without a full understanding of the actual coverage. Conversely, the coverage seems more restricted and limited by exclusions and sub-limits. It's to the point that there is very little coverage for the dollars spent. Seems better to put the dollars toward cybersecurity enhancements and employee training."

Another respondent had harsh words for insurance providers, commenting, "[There has been] increased efficacy of cyber policies with 'some' insurers, but there are far too many woeful, poorly written and ridiculously sub-limited policies being sold, and insurance brokers are a serious problem in not being educated in cyber, and selling on price with no attempt or ability to explain policy terms to clients. We believe that as long as brokers are permitted to sell cyber without cyber policy education and education in cyber breach itself, they are a major threat to their clients and to the insurance industry as a whole, as lack of trust in cyber insurance continues to increase."

These comments highlight the need for brokers to ensure they are well-versed in cyber coverage and have a sufficient understanding of policy elements. When they are, brokers can serve as better insurance partners for risk managers and their associated organizations, providing them with much-needed coverage resources and education in this challenging cyber risk landscape and promoting continued resiliency during difficult market conditions.



A Time of Change for Cyber Insurance Programs

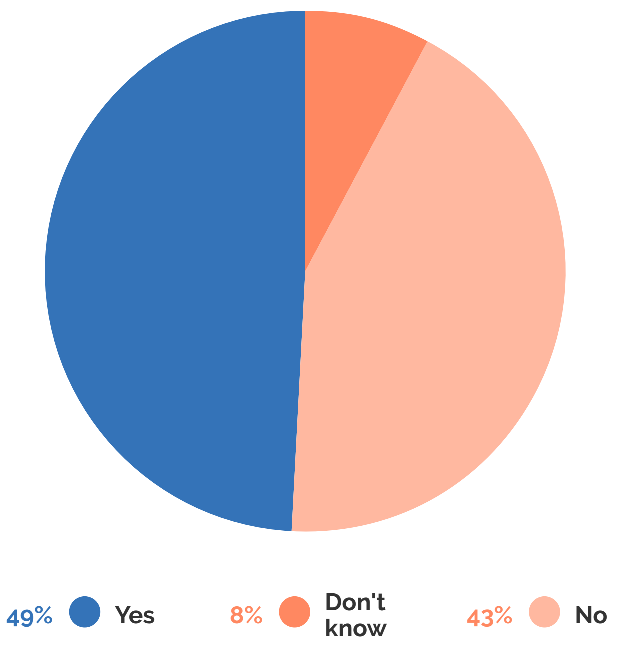
As the market adapts to evolving exposures and increasingly sophisticated attacks, cyber insurance programs have adjusted. Nearly half (49 percent) of respondents reported that they saw changes in the structure of their programs within the past year. Among these respondents, 60 percent said these program changes included increased retentions.

When it comes to modified policy limits, 35 percent of respondents saw increased limits, and 34 percent saw decreased limits. Respondents also voiced difficulties related to putting their programs together, citing issues such as an inability to work with individual carriers, cutbacks on coverage, additional cybersecurity requirements and a lack of transparency from insurance providers. One respondent commented, "We requested higher limits, and for six months now, our broker has not been able to secure higher limits. The retention doubled at renewal, and we were never made aware either. Transparency would have been great."

Another respondent commented on the rigor of underwriters and emphasized that coverage remains available, but for a price. When discussing policy changes following a cyber incident, the respondent commented, "Due to a breach, [our] insurer required multifactor authentication (MFA) and Microsoft Outlook Web Access (OWA), and when our company could not get 100 percent compliant with both, the insurer (1) increased retention by 600 percent, (2) reduced [our] overall limit of insurance, (3) required a co-insurance provision and (4) modified coverage."

One respondent even suggested that ongoing cyber insurance program adjustments have forced their organization to make strategic decisions based on the perceived return on investment (ROI) of coverage, commenting, "[Our insurer] reduced [our policy] limit by 75 percent. Given the cost and uncertainty that coverage would actually apply, [we] would rather expend funds on security enhancements and early detection services."

In the past year did the structure of your cyber insurance program change?

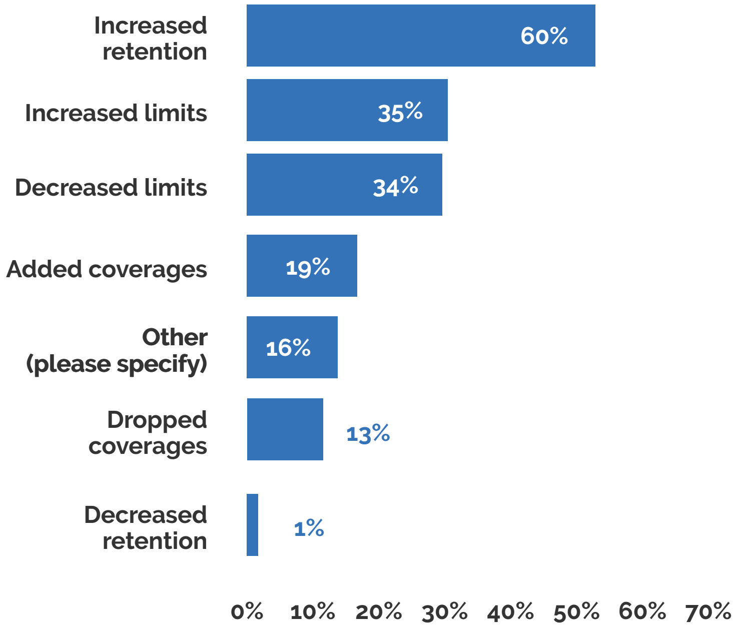


This year's results indicate that cyber insurance has remained fairly broad in some areas. Nearly three-quarters (74 percent) of respondents said their cyber coverage includes protection for cyber-related business interruption losses, and 62 percent said their policies offer such protection for cyber-related contingent business interruption losses. Additionally, 42 percent and 49 percent of respondents said their cyber coverage includes protection for cyber-related property damage losses and funds transfer fraud losses, respectively; further, a small proportion of respondents said they have protection for these losses under different policies.

Yet, a troubling proportion of respondents do not know whether they are covered for these exposures, thus posing the risk of potential policy gaps. In particular, almost one-quarter (22 percent) of respondents said they don't know if their cyber coverage includes protection for cyber-related contingent business interruption losses. Especially with an increase in supply chain incidents and a shift in carriers' willingness to cover vendor outages, such findings warrant concern.

Altogether, these results once again call out the need for brokers to showcase the value of cyber policies and remain informed and able to effectively communicate on potential coverage adjustments, therefore preventing any surprises for insurance buyers—particularly regarding retentions, limits, co-insurance provisions, cybersecurity requirements and overall coverage capabilities. Organizations that are made more knowledgeable about changes to their insurance programs will likely be better equipped to navigate difficult market conditions.

What changed about the structure of your cyber insurance program? (Please select all that apply)

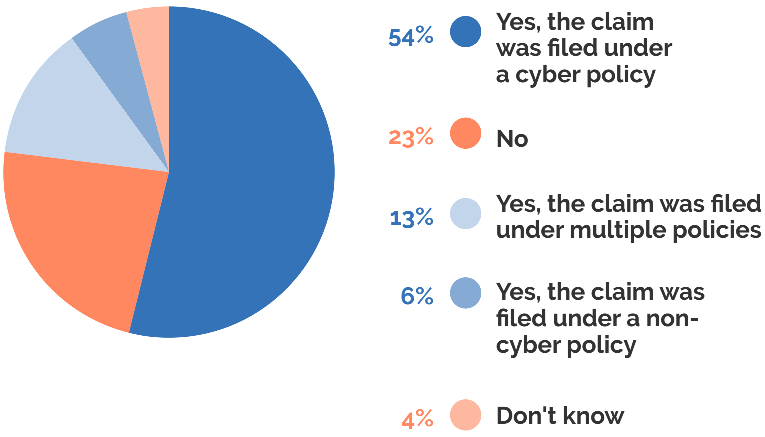


Claims Experience and Satisfaction

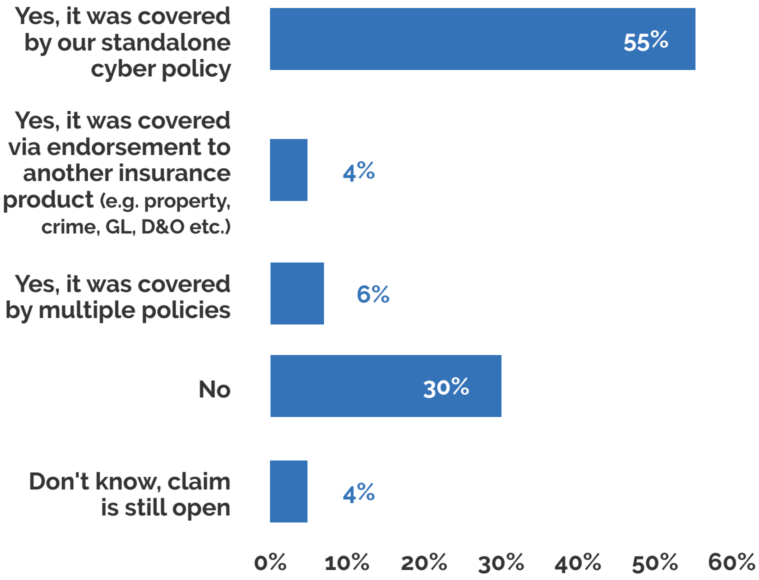
Similar to previous years, this year's results indicate that, despite the increased severity and frequency of cyber incidents, most organizations have yet to experience one themselves or file an associated cyber insurance claim. Almost three-quarters (71 percent) of respondents said they have not faced a cyber event of any kind. Of those who have gone through such an event, 18 percent experienced a data breach, and 6 percent encountered a business interruption incident. Further, 5 percent of respondents said they faced a cyber event encompassing a data breach and business interruption incident.

Among the respondents who experienced a cyber event, more than half (54 percent) filed a claim with their cyber insurance carrier, with 55 percent getting their losses covered by standalone policies and 70 percent recouping costs. (A portion of claims are still being processed.) Nearly one-quarter (23 percent) of respondents did not file claims following cyber events, while 6 percent had their claims covered under multiple policies, and 4 percent received coverage from policies with cyber insurance endorsements.

Did you file a claim with your insurance carrier for the cyber event that resulted in a financial loss?



Did the insurance policy cover the full financial loss sustained by your firm?



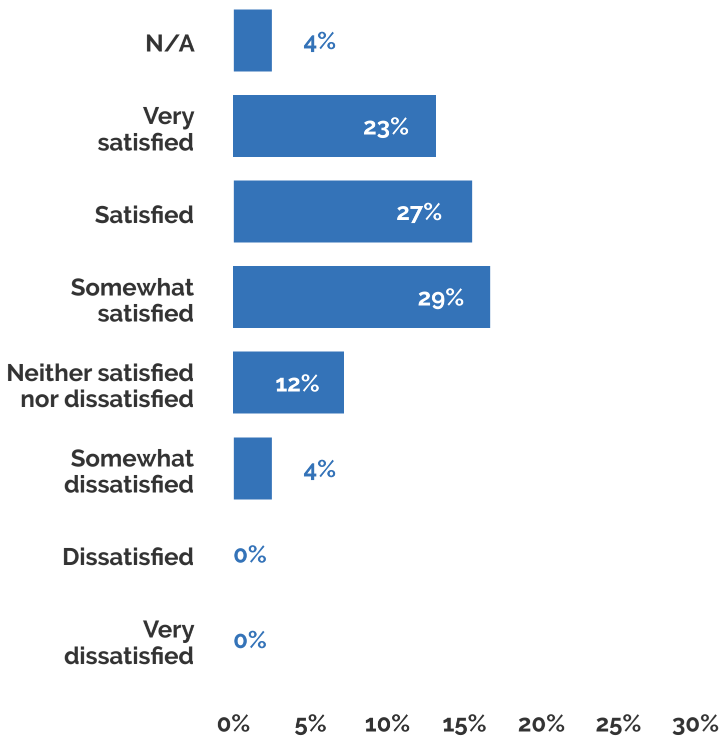
Despite limited cyber claims experience within this year's survey sample, a majority (79 percent) of respondents who had claims paid voiced some level of satisfaction with the claims handling process. More than one-quarter (27 percent) of these respondents said they were satisfied with the process, whereas 23 percent said they were very satisfied, and 29 percent said they were somewhat satisfied. In addition, several respondents praised both their insurance carriers and incident response teams for handling claims effectively—highlighting the value of working with trusted insurance providers and cybersecurity professionals.

Nevertheless, not all respondents had satisfying claims experiences, as evidenced by a handful of negative comments. One respondent shared frustration with rising coverage expenses, commenting, "High retentions mean that businesses have to shoulder more of the burden, even under triple-digit premium increases." Several other respondents called out the timeliness of the claims handling process, mentioning that they have encountered claims negotiations lasting multiple years.

One respondent commented, "My expectation is that insurance for cybersecurity failure events would never result in 100 percent recovery of financial loss of an organization; insurance for 100 percent recovery of loss would be unrealistic/cost-prohibitive. My company's view is that cyber insurance is a financial transfer of catastrophic-level risk only."

Moving forward, even if organizations haven't experienced a large-scale cyber event or filed a cyber insurance claim, they should be fully prepared for these occurrences. Organizations that leverage a collaborative approach to cybersecurity and claims—in which risk managers and insurance providers work together to both prevent and efficiently manage claims—will be better positioned to keep related costs under control.

How satisfied were you with the outcome of the claims process?



Conclusion

Overall, this year's results—namely, the rising uptake in cyber insurance and the increase in cyber risk mitigation efforts—suggest that organizations are more prepared than in the past for potential cyber threats. However, the growing sophistication of attackers and other factors continue to challenge the cyber risk landscape and insurance space.

As so-called "hard market" conditions persist, there are several questions to consider. For instance, how will the market impact organizations that continue to lack cyber risk awareness and resilience going forward? Will a greater line be drawn between organizations that are resilient and those that are not when it comes to cyber coverage eligibility? Amid the rising interconnectivity of society, could this cause organizations that believe they are more prepared for cyber threats to become increasingly vulnerable? And what responsibilities do more resilient, sophisticated organizations have to the general public?

Regardless of the answers to these questions, one thing is certain: Increased thought leadership and shared knowledge regarding cyber risk are absolutely part of the solution. By promoting open communication and prioritizing ongoing education across the cyber insurance space, insurers and brokers can effectively work with organizations to mitigate potential losses and take steps toward resilience.

Methodology

For 12 consecutive years, Zurich North America and Advisen, a Zywave company, have collaborated on a survey designed to gain insight into the trends and current state of cyber risk management. Invitations to participate were distributed by email to risk managers, insurance buyers and other risk professionals. The survey was completed at least in part by 353 respondents. The majority classified themselves as either a chief risk manager or the head of a risk management department (28 percent); a different member of a risk management department (25 percent); a chief information security officer or chief privacy officer (5 percent); or other executive, such as a CIO, CFO or CEO (20 percent).

Leaders from organizations representing a broad range of industries and sizes responded to this year's survey. Those within the finance, banking and insurance sector had the highest representation, constituting one-quarter (25 percent) of total respondents. While every sector listed was selected by at least one survey respondent, industries with significant representation included professional services (8 percent), manufacturing (8 percent), construction (7 percent), healthcare (7 percent) and educational institutions (6 percent). In addition, 11 percent of respondents selected "other" as their industry. Among these respondents, many belonged to the government/municipality and nonprofit sectors.

In terms of size, 22 percent of respondents were from smaller organizations with less than $25 million in revenue. More than one-third of respondents (40 percent) belonged to middle-market organizations with between $25 million and $1 billion in revenue, while 26 percent were from larger organizations with between $1 billion and $10 billion in revenue. An additional 12 percent of respondents belonged to organizations with greater than $10 billion in revenue.